News from Ed Markey

United States Congress **Massachusetts Seventh District**
FOR IMMEDIATE RELEASE **CONTACT: Mark Bayer**
June 16, 2004 **202-225-2836**

MARKEY PERSONAL PRIVACY BILL MADE PART OF HOUSE DEMOCRATIC OFF-SHORING INITIATIVE

LAWMAKER RELEASES LETTERS FROM HHS, FINANCIAL SERVICES REGULATORS SHOWING WEAKNESSES IN CURRENT PRIVACY PROTECTIONS

WASHINGTON, D.C. – Representative Edward J. Markey (D-MA), a senior Democratic Member of the House Energy and Commerce Committee, and the Co-Chair of the Congressional Privacy Caucus, today praised the House leadership for a new Democractic strategy to save jobs which includes protections to protect personally-identifiably data from being shipped abroad without consent. Rep. Markey has introduced H.R. 4366, the "Personal Data Offshoring Protection Act of 2004," to give consumers an opportunity to object to the offshoring of their private data, which often ends up in countries with extrememly weak or nonexistent privacy protections.

"I'm pleased that this issue is receiving the priority it deserves," said Markey. "Leader Pelosi, Representative Miller, and other Democratic Members are helping to alert the public and the press to the dangers of the unregulated offshoring of medical, financial, tax return, and other highly personal data. Current law provides uneven protections from companies transferring a families' most personal information to overseas contractors or subcontractors."

In connection with this announcement, Rep. Markey also released letters he had received from the Department of Health and Human Services, the Federal Deposit Insurance Corporation (FDIC), and a joint letter from federal banking regulators that he pointed to as further evidence of the need for Congress to enacte his personal data offshoring bill.

In the HHS letter, Secretary Tommy Thompson reported that "Neither HIPAA nor the [HHS] Privacy Rule require covered entities or business associates to register with the Department or to report on the nature or content of their contractual relationships." He added, "Thus, we cannot respond to the various requests of your office for data about these relationships." Secretary Thompson also noted that under HIPAA, consumers whose medical privacy has been offshored to an entity which then compromised the confidentiality of their medical records have no right to sue either the U.S. company that transferred the data or the offshore company that released it. The Department's response also indicated that HHS's enforcement efforts are driven entirely by consumer complaints or press reports about potential privacy violations, and that the Department does not conduct routine compliance oversight to determine whether the HIPAA privacy rules are being complied with.

In the FDIC response, Chairman Donald E. Powell provided a copy of an FDIC study on the consumer privacy risks of offshoring of personal data by banks insured by the FDIC. This study reported that "the more complicated chain of control incurred when offshoring financial services and related data may create new risks when compared to domestic outsourcing." The FDIC study further noted that "geographic distance from the function and timing lags in reporting heighten the potential risk exposures." The FDIC found that "few legal restrictions exist on financial services companies sending consumer data to foreign countries," and that "customers may not opt out of these information transfers to nonaffiliated service providers" under loopholes contained the Gramm-Leach-Bliley (GLBA) for data transfers to service providers. In response to these risks, the FDIC made two recommendations: 1) that financial institutions be required to identify currently undisclosed third-party contracting arrangements that their third-party contractors may enter into, and 2) that financial institutions should be required by federal regulation to create a central database of information about all of their outsourcing arrangements, so that regulators could better monitor these arrangements.

The banking regulators letter, which was signed by the heads of the Federal Reserve, the FDIC, the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), reported that "our principal supervisory strategy in this area is to focus on the ability and obligation of the financial institution to maintain controls over the privacy and security practices of its foreign-based service providers that possess or have access to its customer information." The banking regulators stated that they believed this approach was "adequate to protect the privacy and security interests" of U.S. banking customers, although they admitted that none of the agencies collected information on what U.S. banks are currently transferring information about their customers to foreign companies, who they are transferring this data to, for what purpose the information is being transferred, or whether the consumer is given any rights to opt-on or opt-out to such transfers. In addition, the federal banking regulators were also unable to report on how many examinations they had conducted to determine whether outsourcing of consumer information may have resulted in unauthorized disclosure of data. The banking regulators also confirmed that U.S. consumers currently have no legal right under federal law to sue a bank for transferring their personal financial information to an offshore entity who releases this information.

"The letters I have received from HHS and the banking regulators only serve to underscore how weak current federal privacy protections are," concluded Rep. Markey, noting that "Consumers should have a right to know if their personal information is being transferred abroad and a right to say 'No' to this practice if they object."

Copies of the letters Rep. Markey released today can be found at www.house.gov/markey.

***